10–15 FEBRUARY
2023 YEAR

XII INTERNATIONAL

SCIENTIFIC AND PRACTICAL CONFERENCE

SCIENCE AND EDUCATION IN THE MODERN WORLD: CHALLENGES OF THE XXI CENTURY

Astana, Kazakhstan

ОБЪЕДИНЕНИЕ ЮРИДИЧЕСКИХ ЛИЦ В ФОРМЕ АССОЦИАЦИИ «ОБЩЕНАЦИОНАЛЬНОЕ ДВИЖЕНИЕ «БОБЕК»
КОНГРЕСС УЧЕНЫХ КАЗАХСТАНА

«SCIENCE AND EDUCATION IN THE MODERN WORLD: CHALLENGES OF THE XXI CENTURY»

атты XII Халықаралық ғылыми-тәжірибелік конференция

ЖИНАҒЫ

МАТЕРИАЛЫ

XII Международной научно-практической конференции

«НАУКА И ОБРАЗОВАНИЕ В СОВРЕМЕННОМ МИРЕ: ВЫЗОВЫ XXI века»

4. ТЕХНИЧЕСКИЕ НАУКИ

IV ТОМ

АСТАНА – 2023

УДК 378 (063)
ББК 74.58
С 940

С 940
«SCIENCE AND EDUCATION IN THE MODERN WORLD: CHALLENGES OF THE XXI CENTURY» материалы XII Международной науч-прак. конф. (ТЕХНИЧЕСКИЕ НАУКИ)/ сост.: Е. Ешім. – Астана, 2023 – 75 с.

ISBN 978-601-332-271-1

«SCIENCE AND EDUCATION IN THE MODERN WORLD: CHALLENGES OF THE XXI CENTURY» атты XII Халықаралық ғылыми-тәжірибелік конференция материалдары жинағына Қазақстан, Ресей, Қытай, Түркия, Белорус, Украина, Молдова, Қырғызстан, Өзбекстан, Тәжікстан, Түрікменстан, Грузия, Монғолия жоғары оқу орындары мен ғылыми мекемелердің қызметкерлері мен ұстаздары, магистранттары, студенттері және мектеп мұғалімдерінің баяндамалары енгізілді. Жинақтың материалдары жоғары оқу орнындары мен ғылыми мекемелердегі қызметкерлерге, оқытушыларға, мектеп және колледж мұғалімдеріне, магистранттар мен студенттерге арналған.

XII Международная научно-практическая конференция **«НАУКА И ОБРАЗОВАНИЕ В СОВРЕМЕННОМ МИРЕ: ВЫЗОВЫ XXI века»**, включают доклады ученых, студентов, магистрантов и учителей школ из разных стран (Казахстан, Россия, Китай, Турция, Белорусь, Украина, Кыргызстан, Узбекистан, Таджикистан, Молдавия, Туркменистан, Грузия, Монголия). Материалы сборника будут интересны научным сотрудникам, преподавателям, учителям средних школ, колледжей, магистрантам, студентам учебных и научных учреждений.

УДК 378 (063)
ББК 74.58

ISBN 978-601-332-271-1

УДК 535.513.1

SYMMETRIC ENCRYPTION IN KEY DISTRIBUTION PROBLEM BY QUANTUM CRYPTOGRAPHY METHOD

Shukhrat Toirov, Eldor Umarov, Orzu Rajabov
Teacher of Samarkand branch of Tashkent University of Information Technology,
Samarkand, Uzbekistan

Abstract. *This work presents a minimal set of quantum physics concepts necessary to understand the ideas and tools of quantum cryptography. The priority areas of the development of quantum cryptographic distribution systems based on the coding of the quantum state of a single particle are described. Based on the laws of quantum mechanics, the structure of secure data transfer protocols, called quantum protocols of data transfer, is described. In this study, quantum data transmission protocols were considered.*

Keywords: *quantum information theory, quantum cryptography, quantum of keys distribution.*

1. Introduction

The main purpose of cryptography is to hide data, this process is usually carried out by encrypting them. Over time, cryptography began to solve other problems similar to encryption in terms of methods of solving them, for example, the creation and distribution of tokens, the problem of audit of parties, etc. In this case, as a result of the coordinated efforts of users, the solution of such problems is called cryptographic protocols [1].

At the beginning of the XX century, it opened up a close connection between Informatics and physics. At first glance, success in solving many problems that are associated only with information technology and Information Protection can only be achieved in a physical way. Before the scientists, there were two main questions [2]: how large are the possibilities of quantum algorithms and how it is possible to create devices that implement these algorithms.

In the 60-ies of the XX century, when information technology and computer technology began to develop rapidly, a new science - quantum information theory was born. He studies quantum mechanical States and their ability to participate in the transmission and processing of data. Quantum theory is a mathematical model of modern understanding of the physical properties of the surrounding world and the physical systems that it consists of [3].

2. Main part

Basic concepts of quantum information theory. Quantum information theory works with quantum states, Studies their properties and laws. This science is built on the concepts of quantum states and wave function. On their basis, such concepts as quantum bit, the collapse of wave function and the Prohibition of cloning are formed.

Let's dwell on each of the concepts in detail.

There are significant differences between quantum and conventional information theory. First of all, the concepts of quantum particles and particles differ from each other. If there are such properties as coordinates, mass and Magnitude in classical physics for a particle that is regarded as some body in space, then it is impossible to determine in quantum physics which part of them is located (Heisenberg’s uncertainty principle). Nevertheless, it was possible to predict their behavior with a certain probability, which can be described only after a complete rejection of the classical physical properties of the system. This led to the introduction of a new concept of principle - "quantum state" [4].

Quantum state is the positive Hermit operator in the N gilbert phase. In other words, it is a complete set of data (physical dimensions) that determines the characteristics of the system. The information identified by the system is directly related to the system itself.

The description of the complex quantum system is based on the superposition principle. Condition-this is the vector size, which in quantum theory is denoted by the sign $|\psi\rangle$.

The first line is based on the encoding of the quantum state of a single particle and is based on a principle, in which two non-orthogonal quantum states can not be distinguished in an absolutely reliable way [6].

It is possible to indicate the state of any two-level quantum-mechanical system as a linear superposition

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

There are $|0\rangle$ and $|1\rangle$ with complex coefficients α and β of the condition, in addition

$$|\alpha|^2 + |\beta|^2 = 1$$

If $|\psi_1, \psi_2\rangle = 0$ condition is not fulfilled, that is, if the condition is orthogonal, then the laws of quantum mechanics do not allow you to reliably distinguish two quantum states

$$|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$$

and

$$|\psi_2\rangle = \alpha|0\rangle + \beta|1\rangle$$

The safety of the first line is based on the theorem that prohibits cloning an unknown quantum state. Due to the integrity and linearity of quantum mechanics, it is impossible to make an exact copy of an unknown quantum state without affecting the initial state. Suppose the sender and receiver use two-level quantum systems to transmit data that encodes the state of these systems. If the attacker violates the storage medium sent by the sender, he measures his condition and sends it to the recipient, then the condition of this tool will be different than before the measurement. Thus, listening to a quantum channel leads to errors in transmission, which can be detected by legitimate users [5].

And in the protocol BB84, it uses four quantum states of photons, the direction of the polarization vector, one of which the sender chooses depending on the transmitted bit: "1" to 90° or 135°, “0 " to 45° or 0°. A pair of quantum states corresponds to $0\left(|0(+)\rangle\right)$and $1\left(|1(+)\rangle\right)$ belongs to the basis"+". The other pair quantum states correspond to $0\left(|0(\times)\rangle\right)$and $1\left(|1(\times)\rangle\right)$ belong to the " × " basis. Inside both bases, the cases are orthogonal, but in different bases the cases are non-paired orthogonal (orthogonality is necessary to identify attempts to obtain information).

The difference of our work from the protocol BB84 is that the process of creating a key is developed at the following stages.

A random number generation is selected by the first client and sent to the service via special IPS and ports.

The second side is also connected to the server through the same IP and port as above, a random number generation sent by the first client generates the numbers chosen. The generated numbers are compared with the numbers created on the basis of the generation of random numbers from the second side and a single key is created. The same created single key yields the key for both sides.

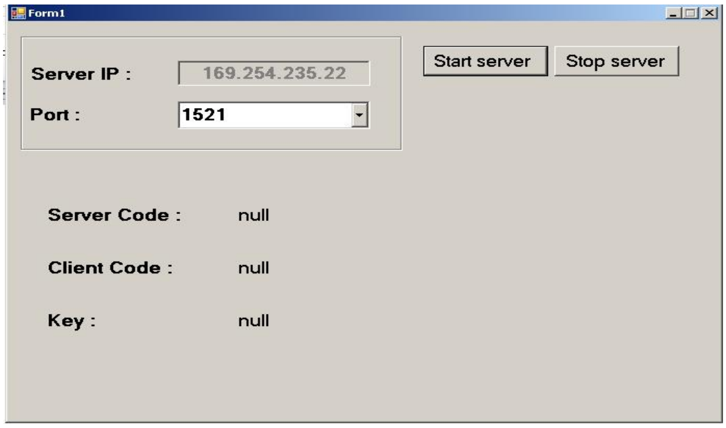
The number of cases in which the selected keys correspond to each other will be equal to the average length of the original sequence, that is, $n = \frac{1}{2}$ [7].

Through quantum cryptography, the key distribution is seen below.

The principle of operation of the key distribution and the analytical software tool created by our principle is as follows.

The value of the program in the IP and port field is selected the address that needs to be calculated [9].

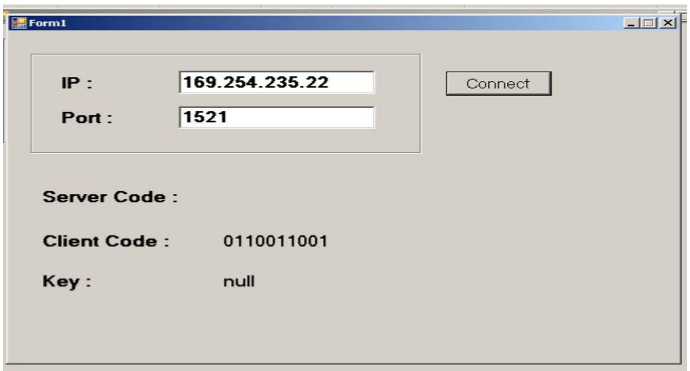
In the Server part, the Start server, the Stop server sections are located.



Server IP : 169.254.235.22
Port : 1521

Server Code : null
Client Code : null
Key : null

1-picture. Server application key allocation

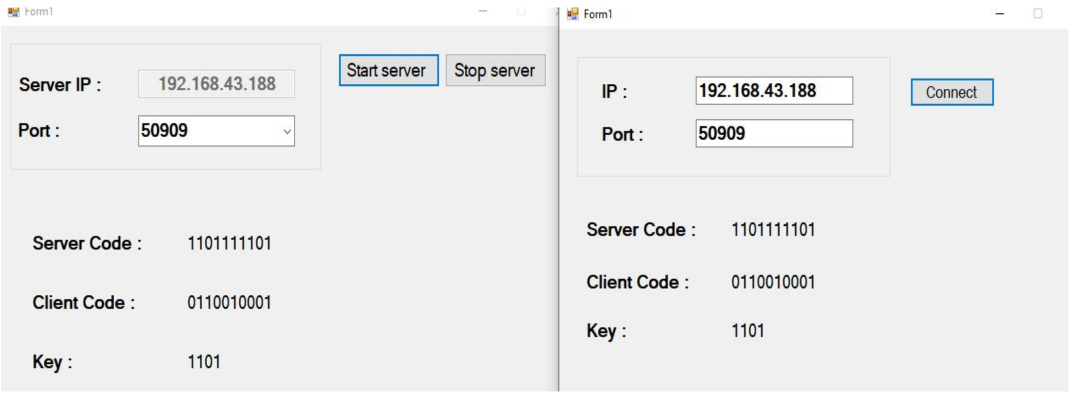


IP : 169.254.235.22
Port : 1521

Server Code :
Client Code : 0110011001
Key : null

2-picture. Determination of address and Port

The client section is located on the IP and Port sections corresponding to the same IP. In the Server side section, keys are generated based on the generation of random numbers chosen by the Server side. In the Client side section, the numbers generated by the client based on the generation of random numbers are written. Key ID is generated from the comparison of the Server and client key while the public single key is generated [8-9].



Server IP : 192.168.43.188
Port : 50909

Server Code : 1101111101
Client Code : 0110010001
Key : 1101

IP : 192.168.43.188
Port : 50909

Server Code : 1101111101
Client Code : 0110010001
Key : 1101

3-picture. Common keys for all

3. Conclusion

At the moment, quantum cryptography is the only alternative to asymmetric encryption systems in the problem of key distribution. In view of the above, in the event of a significant drop in the complexity of hacking asymmetric encryption systems, quantum cryptography has the potential for development.

However, the high technological complexity of the organization of systems using the principles and methods of quantum cryptography does not allow it to displace asymmetric systems even with a sufficiently high level of development of modern technologies.

REFERENCES:

1. Kronberg D.A., Ozhigov Yu.I., Chernyavsky A.Yu. Quantum cryptography//Moscow, Lomonosov Moscow State University Publishing House, 2006, pp. 23-40.

2. Bennett K.H. Quantum cryptography using any two non-orthogonal states//Phys. Rev. Lett., 1992, volume 68, No. 21, pp. 3121-3124.

3. C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing//Institute of Electrical and Electronics Engineers, New York, 1984, pp. 175-179.

4. A. Ekert Quantum cryptography based on Bell's theorem// Phys. Rev. Lett. 67, pp. 661-663 (1991).

5. C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin "Experimental quantum cryptography"// Journal Cryptology 5, pp. 3-28 (1992).

6. A. Muller, J. Breguet, and N. Gisin "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km"// Europhysics Lett. 23, pp. 383-388 (1993).

7. J. Breguet, A. Muller, and N. Gisin "Quantum cryptography with polarized photons in optical fibers: experimental and practical limits"// Journal Mod. Opt. 41, pp. 2405- 2412 (1994).

8. A. Muller, H. Zbinden, and N. Gisin, "Underwater quantum coding"// Nature 378, pp. 449-449 (1995).

9. A. Muller, H. Zbinden, and N. Gisin "Quantum cryptography over 23 km in installed under-lake telecom fiber"// Europhysics Lett. 33, pp. 335-339 (1996).

10. C. Marand and P. Townsend, "Quantum key distribution over distances as long as 30 km"// Opt. Lett., 20, pp. 1695-1697 (1995).

11. P.D. Townsend "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength-division multiplexing"// Electronics Lett. 33, pp. 188-190 (1997).

12. Sh. Toirov. Approaches and algorithms of quantum cryptography// journal “Informatics and Power Engineering”. Toshkent-2020.

13. Sh.Toirov. Effective methods for solving functions using quantum genetic algorithms// XI International Scientific and Practical Conference "Theoretical approaches of fundamental sciences. Theory, Practice and Prospects", April 26-28, 2021, Geneva, Switzerland